DOCUMENTOS
SiC
Nº 25
ABRIL 2018

DXC.technology

Ciberseguridad orientada a la transformación digital

Servicios de ciberseguridad de extremo a extremo adaptados a cada negocio

SC2, protección robusta y gestionada orientada a la transformación digital

Predicciones 2018: el paso de la reacción a la proacción para alcanzar la resiliencia cibernética

Rubén Muñoz
Iberia Security Lead
DXC Technology

DXC Technology: servicios de ciberseguridad de extremo a extremo adaptados a cada negocio

Con un claro foco en asegurar los procesos de transformación digital de las organizaciones, DXC Technology dispone de una oferta bien estructurada de servicios de ciberseguridad de extremo a extremo, que cubre desde el asesoramiento y la consultoría por expertos cualificados hasta la prestación de servicios de seguridad gestionados. Su capacidad de adaptarse a cada tipo de cliente marca el camino a la hora de implementar un enfoque integrado para proteger toda la empresa, asegurando sistemas, puntos finales, usuarios, procesos, aplicaciones y datos de manera efectiva y con independencia tecnológica.


Vista del SC2 ubicado en Madrid.

Bajo un paraguas de más de 35 años de experiencia, DXC Technology ofrece una gama integral de servicios que abarcan desde el asesoramiento de expertos de alto nivel hasta la administración de las operaciones de ciberseguridad. La protección de extremo a extremo para la gestión de infraestructuras, terminales, identidades y redes, así como sus servicios adicionales para proteger aplicaciones y plataformas de nueva generación como la nube, la movilidad, los grandes volúmenes de datos y la analítica avanzada, abanderan su propuesta para ayudar a las empresas a facilitar y agilizar su transformación digital y el crecimiento del negocio.

La independencia tecnológica, la experiencia global y una amplia red de socios y de centros de operaciones son, sin duda, las principales características que hacen que la firma compita con las mejores armas en el mercado. La articulación de más de 4.600 profesionales de seguridad en todo el mundo, cinco Centros de Operaciones de Seguridad (SOC) globales y 11 regionales, soluciones de gestión y monitorización las 24 horas del día, profesionales certificados en las principales tecnologías de ciberseguridad, una base de conocimiento e inteligencia de seguridad global y un conocimiento sectorial profundo, permiten a DXC Technology ofrecer soluciones y servicios de extremo a extremo orientados a la demanda específica del cliente.

En España, la compañía dispone de amplias posibilidades y polivalencias entre centros, también con agentes altamente cualificados y especializados en las distintas áreas de conocimiento, que permiten prestar servicios de excelencia de manera eficiente, tanto desde el punto de vista operativo como financiero. El centro neurálgico para la región de Iberia se ubica pricipalmente en Madrid, donde se erige el Centro de Competencia de Seguridad (SC2) y desde el que DXC Technology ofrece el grueso de sus servicios de ciberseguridad personalizados. Y es que una de las apuestas de la compañía es ofrecer soluciones específicas también de forma sectorizada, cubriendo industrias tan diversas como Banca, Retail, Seguros, Salud, Energéticas, Manufacturing, Logística y Automoción.

La seguridad extremo a extremo para la gestión de infraestructuras, terminales, identidades y redes, así como sus servicios adicionales para proteger aplicaciones y plataformas de nueva generación como la nube, la movilidad, los grandes volúmenes de datos y la analítica avanzada, abanderan la propuesta de ciberseguridad de la compañía.

CATÁLOGO DE SERVICIOS

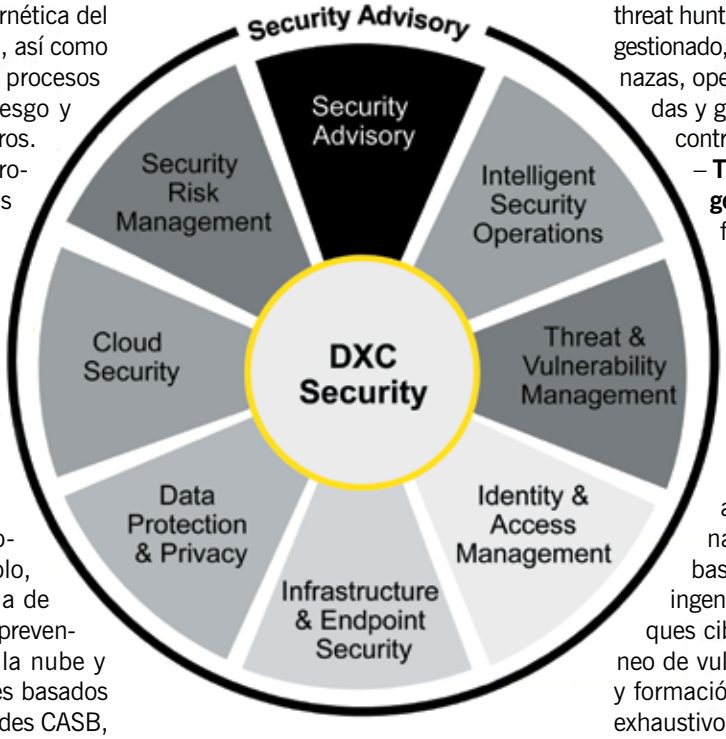
La oferta de servicios de DXC Technology se despliega alrededor de los siguientes frentes de la gestión de la ciberseguridad (ver **Figura 1**):

– Security Risk Management. DXC Technology ofrece servicios de asesoría y gestión para evaluar los riesgos y definir e implementar estrategias y planes alineados con los negocios, así como capacidades de monitorización. Sus servicios de gestión de riesgos incluyen asesoramiento en estrategias de seguridad y transformación, administración de riesgos y cumplimiento, métricas de seguridad,

evaluación de la madurez cibernética del negocio, CISO/DPO provisional, así como asesoría y automatización de procesos de Gobierno Corporativo, Riesgo y Cumplimiento (GRC), entre otros.

– Cloud Security. Con esta propuesta, la compañía dota a las organizaciones de visibilidad del riesgo y las amenazas de seguridad en entornos de aplicaciones en la nube (SaaS) con un proveedor independiente que puede asesorar, transformar y gestionar, incluyendo informes de cumplimiento y respuesta a incidentes. En concreto, los clientes de DXC Technology podrán obtener, por ejemplo, asesoramiento en su estrategia de ciberseguridad en la nube, en prevención de pérdida de datos en la nube y en protección de puntos finales basados en cloud, además de capacidades CASB, seguridad de la nube pública –AWS y Microsoft Azure–, y monitorización de la integridad de archivos.

– Data Protection and Privacy. DXC Technology proporciona a sus clientes una mayor visibilidad y control de la gestión de su información crítica, a través de servicios de protección de datos diseñados, implementados y administrados con ese único fin. Entre los servicios que se ofrecen en este sentido se incluyen: asesoramiento en prevención de pérdida de datos, PKI y servicios de asesoramiento en gestión de certificados, gobierno de datos, cifrado y gestión de derechos, así como prevención de pérdida de datos gestionada, infraestructura de clave pública gestionada y pruebas de validación de módulos y algoritmos criptográficos.



– Intelligent Security Operations. Este servicio ofrece una visión integral de la seguridad en toda la empresa con el fin de reducir el número y la complejidad de los incidentes de seguridad, reforzando las defensas de las compañías. Para ello, DXC Technology proporciona servicios de asesoramiento SIEM, respuesta a incidentes y análisis forense digital, asesoría sobre threat hunting, control de seguridad, SIEM gestionado, inteligencia global contra amenazas, operaciones de seguridad integradas y gestión avanzada de protección contra amenazas, entre otros.

– Threat and Vulnerability Management. Proporciona una identificación regular y proactiva de las vulnerabilidades a través de información dirigida y "accionable" sobre vulnerabilidades y recomendaciones de remediación para evitar que ciberdelincuentes (internos o externos) exploten dichas debilidades. Este servicio incluye asesoría sobre gestión de amenazas y vulnerabilidades, pruebas de penetración o pentesting, ingeniería social, simulación de ataques cibernéticos –Red Team–, escaneo de vulnerabilidades, concienciación y formación en spear phishing, análisis exhaustivo de amenazas de aplicaciones (USPS) y seguridad de aplicaciones bajo demanda.

– Identity and Access Management. A través de este servicio, los clientes de DXC Technology obtienen mayor control y visibilidad de los usuarios y sus privilegios de acceso, mejorando la posición general de la ciberseguridad. Estos servicios incluyen provisión de cuentas, herramientas de gobierno y cumplimiento, herramientas de autenticación y soluciones de políticas de cuentas/contraseñas privilegiadas, autenticación multifactor, gestión de identidades como servicio (IDMaaS) y servicios de federación de identidades, entre otros.

– Infrastructure and Endpoint Security. La compañía completa su cartera de servicios con una gama de soluciones integradas de protección de múltiples capas que monitorizan, detectan y protegen los entornos del cliente frente a amenazas externas e internas. En este frente se incluyen servicios de asesoramiento sobre ciberseguridad de la infraestructura**,** ciberseguridad web y de correo electrónico**,** asesoría en ciberseguridad de servidores y puntos finales**,** cortafuegos de próxima generación (NGFW) y prevención de amenazas, gestión de red IDS/IPS, proxy administrado, servicio de protección frente a ataques DDoS y control del conjunto de reglas de los cortafuegos. ●

Rubén Muñoz

Iberia Security Lead DXC Technology

Como responsable del área de seguridad de DXC Technology para la región de Iberia, Rubén Muñoz desvela la estrategia de la compañía en la prestación de servicios de ciberseguridad como parte de un proceso más amplio que se focaliza en asegurar la transformación digital de las organizaciones, lo que requiere profesionales muy cualificados y una plena orientación al cliente.

"DXC ofrece las ventajas de los servicios globales y estandarizados de seguridad, añadiendo una capa de personalización local"

– DXC sitúa su foco estratégico en ayudar a sus clientes en los procesos de Transformación Digital. ¿Cómo se integran los servicios de ciberseguridad en esa orientación y cuál es el factor diferencial frente a otros jugadores?

– Nuestro valor diferencial es que DXC Technology puede cubrir todas las áreas tecnológicas involucradas en un proceso de transformación digital (cloud, apps, analytics, workplace, cybersecurity), garantizando que la ciberseguridad no es una capa que se aplica en paralelo a la transformación digital, sino que forma parte del core de dicha transformación, entrelazándose con todas las áreas implicadas, no como un vigilante o regulador, sino como parte de un proceso completo.

– ¿Cómo se estructura el área de ciberseguridad de DXC en España y desde España?

– El área de ciberseguridad de DXC en Iberia posee total autonomía operativa y está incluido y respaldado dentro de una organización global de ciberseguridad con más de 4.600 expertos.

A nivel nacional, tenemos una organización que permite un alto grado de especialización y articula de manera efectiva nuestra capacidad extremo a extremo, todo bajo una estrategia coordinada y consolidada a nivel local por mi rol y que está segmentada en los siguientes equipos: Governance & Customer Compliance,

"La ciberseguridad no es una capa que se aplica en paralelo a la transformación digital, sino que forma parte del core de dicha transformación, entrelazándose con todas las áreas implicadas, no como un vigilante o regulador, sino como parte de un proceso completo".

Security Advisory Services y Managed Security Services. Actualmente, contamos con unos 90 profesionales expertos con amplia variedad de certificaciones de seguridad (CISSP, CISM, CISA, Lead Auditor, etc., o certificaciones de fabricantes) y tenemos una previsión de crecimiento para este año de al menos un 50%.

– ¿Qué papel juega el Centro de Competencia de Seguridad (SC2), ubicado en Madrid, en la estructura de servicios de DXC Technology en el mercado español?

– El SC2 garantiza flexibilidad y adaptación a las necesidades de cada cliente, creando así, junto con nuestros SOC globales, una dualidad Global-Local diferenciadora dentro de los servicios de seguridad gestionada del mercado, ya que DXC permite ofrecer las ventajas de servicios globales y estandarizados de seguridad, pero añadiendo una capa de personalización local, combinación que muy pocos proveedores de servicios de seguridad pueden ofrecer actualmente en España. El SC2 juega un papel fundamental en la estrategia de negocio de ciberseguridad en Iberia, dado que la tendencia del mercado en los últimos años ha sido que los clientes demandan, cada vez más, partners de seguridad en modalidad "as a service".

En muchos casos, la demanda está vinculada a la capacidad de poder ofrecer dichos servicios gestionados, es decir, si no tienes una plataforma capaz de ofrecer servicios de seguridad gestionados, no eres elegible para otro tipo de servicios. Por lo tanto, existe una relación directa entre el crecimiento del negocio de ciberseguridad local en DXC Iberia y el crecimiento del SC2. Tal es así que ya hemos empezado a distribuir funcionalidades al equipo de seguridad ubicado en el Global Delivery Center (GDC) de DXC en Avilés, para configurar un nuevo nodo activo de seguridad en Iberia. También os puedo decir que dentro de nuestras líneas de crecimiento, está la creación de un nuevo Centro de Competencia de Seguridad en una nueva localización en Iberia.

– ¿En base a qué criterios seleccionan las tecnologías que constituyen la base de algunos de los servicios de MSSP? ¿Prestan atención a aquellas emergentes y que pueden ayudar a ofrecer servicios disruptivos?

– DXC Technology es una compañía agnóstica en tecnología, por lo que los criterios de selección del área de ciberseguridad en Iberia son la funcionalidad, fiabilidad, eficiencia y eficacia.

Dicho esto, en el ADN de nuestros servicios gestionados está un alto grado de personalización para con nuestros clientes, muestra de ello es la Innovation Factory del SC2, cuya finalidad es diseñar y formalizar nuevos modelos de microservicios sobre la plataforma SC2, surgidos de las necesidades específicas de los clientes, y que los servicios ya implementados no cubren. Dentro de los procesos de esta Innovation Factory, la búsqueda y selección de tecnología disruptiva es fundamental, pero aún en este caso, nos guiamos por los criterios de selección ya comentados.

– ¿Podría mencionar el tipo de proyectos de ciberseguridad que tiene abiertos hoy DXC Technology en el mercado español?

– Algunos ejemplos representativos de servicios en ejecución son: Monitorización y gestión de alertas de seguridad; Administración y operación de infraestructura de seguridad; Consultoría de cumplimiento y adecuación normativa; Protección de aplicaciones; Arquitectura de seguridad; Gobierno y gestión de las identidades y control de acceso de identidades privilegiadas; Protección y privacidad del dato; y Protección del cloud.

Estos proyectos se están ejecutando en diferentes industrias (banca, retail, logística, etc), con el enfoque adecuado para cubrir los requerimientos de cada uno de los clientes. ●

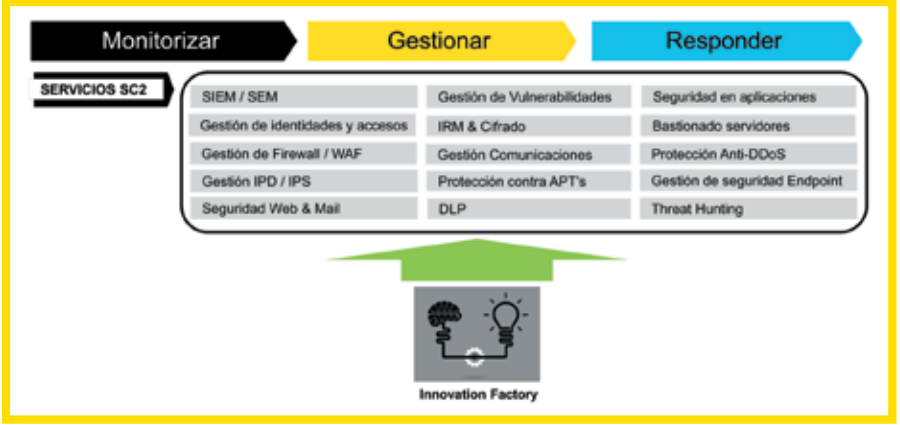
SC2, servicios gestionados robustos y orientados a la transformación digital

La prestación de servicios gestionados desde centros especializados representa una de las líneas de oferta de mayor crecimiento en los últimos años para los diferentes tipos de proveedores (operadores de telecomunicaciones, integradores, consultoras,...), lo que ha provocado, de una parte, un gran avance en su industrialización, y de otra, y como consecuencia, la necesidad de diferenciación de los proveedores.

DXC Technology dispone, a través de su Security Competence Center SC2, ubicado en Madrid, de un catálogo de servicios gestionados dinámico y bien dimensionado para las necesidades estandarizadas de cada cliente. Al tiempo, y como hecho diferencial, brinda capacidades para el desarrollo y prestación de servicios de desarrollo específico y a medida de cada cliente, a través de su Innovation Factory. La personalización es una de las líneas que distinguen a esta multinacional global de TIC, constituyendo uno de los factores de su rápida adaptación a las necesidades de los grandes usuarios, algo esencial para incrustar de forma rápida la ciberseguridad en los servicios y microservicios catapultados por la transformación digital.

Vista del SC2 ubicado en Madrid.

DXC Technology potencia y completa las capacidades de sus clientes antes, durante y tras la transformación digital de su negocio, mediante servicios de ciberseguridad diseñados y adaptados a cada escenario y nivel de madurez.



MEDIOS

DXC Technology dispone en su SC2 de capacidades tecnológicas confiables, propias y de terceros, para monitorizar, operar y administrar la infraestructura de ciberseguridad de sus clientes, además de con un equipo humano con los diferentes perfiles técnicos y de gestión necesarios y contrastables: operadores, técnicos especialistas y analistas para poder cubrir, en el contexto de los servicios, la prevención, la detección de incidentes, la reacción en base al desarrollo de la crisis y el reporte en cada momento y para todos los niveles organizativos establecidos, en los tres frentes cubiertos: monitorización, gestión y respuesta.

El SC2 está pensado para poder hacer frente a situaciones de emergencia en cada cliente de una manera rápida y eficaz gracias a su nivel de adaptación. ●

Ciberseguridad 2018: el paso de la reacción a la proacción para alcanzar la resiliencia cibernética

Toda organización necesita investigar, planificar y reforzarse ante posibles ataques y amenazas cibernéticas, porque estos incidentes, tarde o temprano, sucederán. Sin embargo, la mayoría de las organizaciones siguen en un estado reactivo y es algo que debe cambiar. Para DXC Technology es la hora de evolucionar hacia un modo proactivo. Para ello, la compañía ha elaborado un informe con las 10 predicciones en seguridad que marcarán el año 2018, acompañadas de una serie de recomendaciones para responder a estos nuevos desafíos con el fin de proteger a las empresas en su viaje hacía la transformación digital, la resiliencia cibernética y la protección de sus activos más críticos.

1. **La ciberguerra se intensifica**. Ante el aumento progresivo de las capacidades cibernéticas ofensivas de los Estados-nación, las organizaciones deben adoptar una postura de "compromiso asumido". Para DXC esto refuerza la necesidad de establecer una defensa en profundidad para minimizar los puntos más vulnerables y reducir el riesgo, con revisiones periódicas del grado de madurez de sus cibercapacidades.
2. **El ransomware gana sofisticación**. Los incidentes por ransomware son cada vez más frecuentes y sofisticados. DXC recomienda dotarse de resiliencia con diversas técnicas de prevención que incluyen detección temprana y segmentación de la red, fortalecimiento de los puntos finales, detección de intrusiones en el host, respuesta a incidentes y administración de parches. Además, es importante concienciar y formar a los empleados en este sentido.
3. **La aplicación de parches puede generar frustración**. El desarrollo de parches puede afectar a la alta disponibilidad de los sistemas de TI. Sin embargo, siguen siendo una parte importante de la gestión de vulnerabilidades. Para DXC, las organizaciones deben analizar minuciosamente el desarrollo de aplicaciones y proporcionar un entorno operativo constante y estable para el parcheado automático, junto con programas DevSecOps estructurados.
4. **La informática sin servidor sesga la seguridad**. Las arquitecturas sin servidor o serverless computing es una tendencia creciente en la nube, donde los requisitos de seguridad cambian. Para garantizar que la seguridad sigue siendo relevante, DXC recomienda a las empresas centrarse en la protección de aplicaciones, promover prácticas DevSecOps e invertir en capacitación y manejo de datos. Además, es importante realizar pruebas de pentesting periódicas y utilizar cortafuegos de aplicaciones web.
5. **IoT difumina los límites**. Para evitarlo, DXC recomienda preparar un marco claro para gestionar la introducción del IoT a escala y desarrollar la seguridad al inicio de cualquier proyecto de desarrollo de software. Otros enfoques clave incluyen la seguridad en la virtualización, controles criptográficos robustos, así como llevar a cabo simulaciones de ataques en los sistemas IoT y controlar el crecimiento del shadow IT.
6. **El CISO despliega un ejército de clones**. Los CISOs se están reposicionando en la empresa desplegando la seguridad por diferentes departamentos. DXC recomienda que, antes de implementar la seguridad en otras áreas funcionales, se considere si la seguridad de la información aún satisface las necesidades de su organización. Asimismo, destaca vincular la seguridad con las funciones comerciales, fomentando un uso más amplio de la tecnología para mejorar la productividad empresarial.
7. **El robo de credenciales se automatiza**. Las credenciales continúan siendo un punto de entrada privilegiado para los ciberdelincuentes. Desde la perspectiva de DXC, las organizaciones deben esforzarse por hacer de 2018 el año de la identidad. Esto significa adoptar nuevas prácticas –como usar contraseñas locales diferentes, crear niveles mínimos de privilegios, etc.–, y prepararse para aumentar la demanda de identidades generadas por los dispositivos IoT.
8. **El SOC está muerto o viva el SOC**. La misión del SOC es vital: detectar y responder a las amenazas. Desafortunadamente, la mayoría de los SOC adolecen de grandes volúmenes de tráfico y escasez de personal cualificado. Para DXC, las organizaciones inteligentes crearán un SOC de próxima generación y servicios relacionados fomentando la colaboración entre el SOC y el negocio. También, es importante automatizar la recopilación y el análisis de datos.
9. **Los ciberataques son más intensos**. Ante esta problemática, las organizaciones deben, especialmente, tomar conciencia del valor de sus activos comerciales, evaluar las nuevas y viejas amenazas a las que se pueden enfrentar y, finalmente, administrar estos riesgos de acuerdo con su "apetito" y presupuesto.
10. **Las criptomonedas como objetivos de ataque**. Desde la perspectiva de DXC, estos nuevos riesgos deben ser evaluados por los equipos de riesgo de una organización de las áreas de Finanzas, Operaciones e Informática. Las empresas deben mantenerse al día con los últimos avances en este ámbito, incluyendo los avances en áreas como la computación cuántica, el silicio y los ataques específicos de algoritmo.